



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,294	02/05/2002	George Robert Blakley	LYRN002US0	9653

37141 7590 09/19/2005

FORTKORT GREATHER + KELTON LLP
8911 N. CAPITAL OF TEXAS HWY.
SUITE 3200
AUSTIN, TX 78759

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/068,294

Applicant(s)

BLAKLEY ET AL.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 January 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 7-11, 17-21 and 26-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 7-11, 17-21, and 26-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claims 7-11,17-21, and 26-31 have been considered.

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 7-9 and 17-19 are drawn to a method for encrypting data using a modulus C that is w-big and w-heavy, classified in class 713, subclass 168 (Electrical Computers and Digital Processing Systems: Multiple Computer Communication Using Cryptography: Particular Communication Authentication Technique). The applicant has disclosed that w-big and w-heavy are distinct with respect to w-little and w-light and provided distinguishing definitions for w-big and w-heavy (Specification: page 20).

II. Claims 10-11 and 20-21 are drawn to a method for encrypting data using a modulus C that is w-little and w-light, classified in class 713, subclass 168 (Electrical Computers and Digital Processing Systems: Multiple Computer Communication Using Cryptography: Particular Communication Authentication Technique).

III. Claims 26-29 are directed to a method for hashing data using a modulus C that is w-big and w-heavy, classified in class 713, subclass 181 (Electrical Computers and Digital Processing Systems: Multiple Computer Communication Using Cryptography: Particular Communication Authentication Technique: Message Digest Travels with Message).

IV. Claims 30-31 are directed to a method for hashing data using a modulus C that is w-little and w-light, classified in class 713, subclass 181 (Electrical Computers and Digital Processing Systems: Multiple Computer Communication Using Cryptography: Particular Communication Authentication Technique: Message Digest Travels with Message).

The inventions are distinct each from each other because:

Inventions I,II,III, and IV are related as subcombinations.

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, a method of encrypting data using a computed C-modulus that is w-big and w-heavy (I) is different from a method of encrypting data using a computed C-modulus that is w-little and w-light (II). The applicant has defined w-big and w-heavy to be distinct from w-little and w-light (Specification: page 20). Furthermore, the applicant discloses that the inventions are separately usable: "Some embodiments achieve computational advantages by using a castout modulus that is both w-big and w-heavy. Some embodiments achieve computational advantages by using a castout modulus that is both w-little and w-light" (Specification: page 20). For at least these reasons, the subcombinations are separately usable and therefore restriction is proper. See MPEP 806.04(b).

Inventions I and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, a method of encrypting data (I) is separately usable from a method of hashing data (III). See MPEP 806.04(b).

Inventions I and IV are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, a method of encrypting data (I) is separately usable from a method of hashing data (IV). See MPEP 806.04(b).

Inventions II and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, a method of encrypting data (II) is separately usable from a method of hashing data (III). See MPEP 806.04(b).

Inventions II and IV are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, a method of encrypting data (II) is separately usable from a method of hashing data (IV). See MPEP 806.04(b).

Art Unit: 2137

Inventions III and IV are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, a method of hashing data using a computed C-modulus that is w-big and w-heavy (III) is different from a method of hashing data using a computed C-modulus that is w-little and w-light (IV). Furthermore, the applicant discloses that the inventions are separately usable: "Some embodiments achieve computational advantages by using a castout modulus that is both w-big and w-heavy. Some embodiments achieve computational advantages by using a castout modulus that is both w-little and w-light" (Specification: page 20). For at least these reasons, the subcombinations are separately usable and therefore restriction is proper. See MPEP 806.04(b).

Because the inventions are distinct for the reasons given and have acquired a separate status in the art and require a separate search strategy in the art, restriction for examination purposes is proper. A complete response to this requirement must include an election of the invention to be examined even if the requirement is traversed.

Conclusion

A shortened statutory period for response is set to expire one month (not less than 30 days) from the mail date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C. 133, MPEP 710.02, 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
5 you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

10